ABSTRACT OF THE DISCLOSURE

A Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the apparatus is allowed to utilize cryptanalysis conditions held at given predetermined steps, and decryption with higher order differences determined from stirred text at these steps is allowed. The invention can secure all the estimated extended keys including the last-step extended key to be right with a desired probability as well as it allows decryption by less complexity. The invention allows MISTY1 with six rounds without an FL function to be decrypted with 2^{39} of selected plaintext and the complexity of 2^{49} of an FO function. It also allows MISTY1 with seven rounds without the FL function to be decrypted with 2^{39} of selected plaintext and the complexity of 2^{124} of the FO function.